REMARKS

By this amendment, claims 1-17 are pending, in which claims 1 and 17 are currently amended. No new matter is introduced.

The Office Action mailed September 9, 2004 rejected claims 1-17 under 35 U.S.C. § 102 as anticipated by *Matyas et al.* (US 5,200,999). This rejection is respectfully traversed because *Matyas et al.* does not disclose the features of the claims.

For example, independent claim 1, as amended, recites, and dependent claims 2-12 incorporate pursuant to 35 U.S.C. § 112, ¶ 4, three different digital signatures of three different **contents** (in **bold**) with three different *private keys* (in *italics*):

> 1. (Previously Presented) A method for authenticating transmitted data in real time, the method comprising the steps of:
> (a) generating a master cryptographic key pair, including a first public key and a first private key;
> (b) publishing a first certificate issued by a certificate authority, the first certificate including the first public key and **a first digital signature of the first public key** *based on a private key from the certificate authority*;
> (c) generating a disposable cryptographic key pair, including a second public key and second private key;
> (d) generating a second certificate, the second certificate including the second public key and **a second digital signature of the second public key** *based on the first private key*;
> (e) publishing the second certificate;
> (f) **signing data to be transmitted with a third digital signature** by processing the data to be transmitted through a first one way hashing function to generate a first hash value and encrypting the first hash value *utilizing the second private key*;
> (g) processing received data through the first one way hashing function to create a second hash value;
> (h) decrypting the received third digital signature utilizing the second public key to obtain a third hash value; and
> (i) verifying authenticity of the received data by comparing the second hash value to the third hash value,
> wherein the first private key, the second private key, and the private key from the certificate authority have different values.

This feature is not shown in *Matyas et al.* *Matyas et al.* merely mentions a PR2 master key "used to generate an authentication signature for the public and private keys kept outside the

cryptographic facility" (col. 9:47-50), but *Matyas et al.* fails to describe a system with "a first digital signature of **the first public key** based on *a private key from the certificate authority*" and "a second digital signature of **the second public key** based on *the first private key*" in which "wherein the first private key, the second private key, and the private key from the certificate authority have different values" as recited in claim 1. In fact, *Matyas et al.* does not even describe digital signatures "based on a private key from the certificate authority."

The passages of *Matyas et al.* cited in the Office Action, namely cols. 12:28–13:9 and 24:43–26:14, do not support the rejection because there is no description there of a digital signature for a public key.

Furthermore, independent claim 13 recites the following features:

> (b) publishing a first certificate, the first certificate including the first public key and a first digital signature based on *a key pair of a certificate authority*;
> (c) generating a disposable key pair, the disposable key pair including a second public key and a second private key, and **wherein the disposable key pair is shorter than the master key pair**;
> (d) generating a second certificate, the second certificate including the second public key and a second digital signature *based on the master key pair*;
> (g) encrypting the hash value utilizing the *second private key* as the encryption key; and

Matyas et al. does not disclose this feature because only the PR2 master key is used to generate signatures in the *Matyas et al.* system, and there is no disclosure of "disposable key pair" used to generate the recited second digital signature in *Matyas et al.* that is "shorter than" the PR2 master key.

Accordingly, independent claim 15, which recites "a digital signature of the short public key based on a long private key longer than the short private key," is also patentable over *Matyas et al.*—as are independent claim 14 ("a short disposable key pair that is shorter than the long

master key pair") and independent claim 16 ("wherein the short public key is shorter than the long public key").

Independent claim 17, as amended, sets forth "verifying the first public key based on a digital signature of a second public key issued by a certificate authority and having a different value than the first public key." For the reasons described above, nothing in *Matyas et al.*, including the PR2 master key, satisfies this feature.

Therefore, the present application, as amended, overcomes the objections and rejections of record and is in condition for allowance. Favorable consideration is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at 703-425-8516 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

DITTHAVONG & CARLSON, P.C.

12/7/2004
Date

Stephen C. Carlson
Attorney/Agent for Applicant(s)
Reg. No. 39929

10507 Braddock Road
Suite A
Fairfax, VA 22032
Tel. 703-425-8516
Fax. 703-425-8518